(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 130 491 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.09.2001 Bulletin 2001/36

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **00310771.1**

(22) Date of filing: **04.12.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **14.01.2000 US 483189**

(71) Applicant: **Hewlett-Packard Company, A Delaware Corporation
Palo Alto, CA 94304 (US)**

(72) Inventor: **Corella, Francisco
Hayward, California 94541 (US)**

(74) Representative: **Jehan, Robert et al
Williams, Powell & Associates,
4 St Paul's Churchyard
London EC4M 8AY (GB)**

(54) Digital certificate including authorization data

(57) A structured digital certificate (30) includes a hierarchy of folders (38-44). Each folder (38-44) contains authorization information for a specific relying party, such that a single structured digital certificate (30) can be used by multiple relying parties. A hash of the digital certificate is computed, and each folder contributes the hash of its authorization information rather than the authorization information relevant to the overall hash. The structured digital certificate (30) is presentable to a relying party in a state where only the authorization information relevant to the relying party is visible to the relying party, because the authorization information of unrelated folders are replaced by the hash of the authorization information.

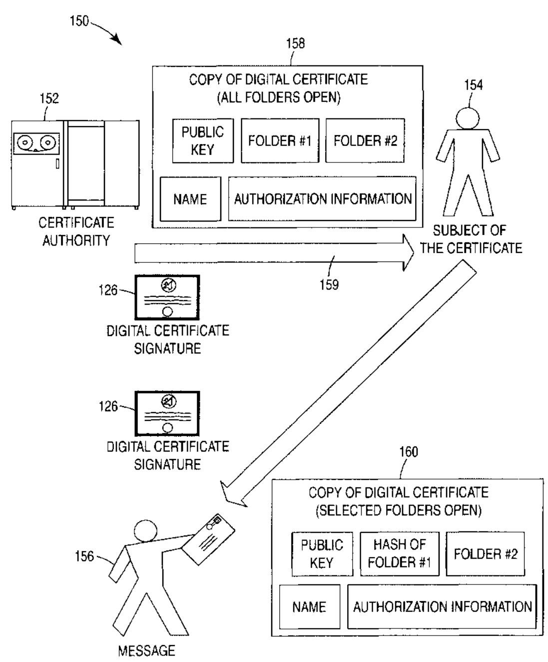

Fig. 6

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] This patent application is related to the following Non-Provisional U.S. Patent Applications: Serial Number 09/483,185 , entitled "AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY," Serial Number 09/483,356, entitled "LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING DISPOSABLE CERTIFICATES," and Serial Number 09/483,186, entitled "LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES," and the following Provisional U.S. Patent Application Serial Number 60/176,157, entitled "PUBLIC KEY VALIDATION SERVICE," which were all filed on even date herewith, are all assigned to the same assignee as the present application.

[0002] The present invention relates to verifying an entity's identity and/or capabilities on a data network, and more particularly, to an apparatus and method for using hierarchically structured digital certificates containing authorization information to verify the identity and/or capabilities of an entity on a data network.

[0003] In everyday life, trust is granted between individuals based on characteristics defining the relationship of the individuals and the identity of the individual in question, such as familiarity, occupation, status, and third party voucher of the individual in question. However, trust between individuals communicating on a public internet is not typically granted in such a simple and straightforward manner, because individuals can assume almost any identity in cyberspace. While the public internet offers flexibility and freedom, the public internet also instills high levels of distrust, especially when granting authority to an individual or when transmitting private, sensitive, or confidential information.

[0004] On the public internet, a digital certificate is typically used to verify the identity and/or capabilities of a subject or sender of the digital certificate presented to a recipient or relying party of the digital certificate. A third party, referred to as a certificate authority or issuer of the digital certificate, researches the subject/sender desiring certification, and issues a digital certificate to the subject/sender to vouch that the subject/sender of the message is actually who they say they are. The certificate authority digitally signs the digital certificate. The subject of the digital certificate presents the signed digital certificate to the relying party who trusts the certificate authority. The relying party computes a cryptographic hash of contents of the digital certificate and uses the cryptographic hash together with a certificate authority's public key, which is readily available, to verify the digital signature. The verification of the digital signature verifies that the digital certificate was issued by the certificate authority.

[0005] Basic public key digital certificates contain a public key and a name associated with the sender. Extended public key certificates typically contain additional fields of authorization information not found in the basic public key certificates. Authorization certificates omit the name, and bind the public key directly to authorization information. Attribute certificates omit the public key, and bind the name to authorization information.

[0006] Currently, the leading digital certificate standard is X.509 version 3 (X.509v3). The X.509v3 standard is an extended public key certificate standard, which can contain additional fields of authorization information not found in the basic public key certificates. The X.509v3 standard supports Secure Sockets Layer 3.0 encryption along with other encryption schemes. Both Netscape Communicator 4.0 and Microsoft's Internet Explorer 4.0 support X509v3 certificates.

[0007] In X.509v3 digital certificates, each extension field has a criticality flag. The criticality flag is employed in situations where the recipient of a digital certificate is presented with one or more extension fields within the digital certificate that the recipient does not understand, perhaps because the extension field is newer than the computer program used by the recipient. If the criticality flag is not set, the recipient can ignore the unknown extension field. If the criticality flag is set, the relying party must reject the digital certificate.

[0008] In certain situations, it is convenient to collect information intended for multiple uses in the same digital certificate by using two or more unrelated fields within the digital certificate. This approach provides the simplicity of a single digital certificate for a wide variety of authentication and authorization needs. This approach, however, compromises confidentiality since all recipients have access to all fields, related or unrelated to the recipient's requirements. For example, a single digital certificate may grant access to a Unix platform and also grant permission to sign purchase orders. In this example, the digital certificate has first type fields that specify a user ID and group ID for the Unix platform, as well as second type fields that specify a limit on the value of purchase orders that the recipient of the digital certificate is authorized to sign. Thus, when the digital certificate is used to access the Unix platform, the second type fields (i.e., the purchase order limit) are unrelated to the recipient's requirements and may become visible to the Unix administrator, such as by being recorded on the system log. The Unix administrator has no need to know the limit on the value of purchase orders, and it would be best if this purchase order information were not disclosed unnecessarily.

[0009] Alternative approaches have been developed to work around the confidentiality problem that results from two or more unrelated fields residing within the same digital certificate. In a first alternative approach, confidentiality is achieved by encrypting some or all of the fields of the digital certificate. The first alternative approach only provides protection against a third party that eavesdrops on the transmission of the digital certificate to the relying party. This first alternative approach cannot provide confidentiality against the recipient itself, because the recipient needs access to the plaintext of

the entire digital certificate in order to compute a cryptographic hash necessary to validate the digital certificate.

[0010] In a second alternative approach, the sender uses separate digital certificates instead of placing information in multiple, unrelated fields within a single digital certificate. For example, instead of using one digital certificate containing the public key and the name of the sender together with three types of fields containing authorization information for three unrelated applications, the second alternative approach uses four separate digital certificates. The four separate digital certificates include a first basic public key certificate binding the public key to the sender name, and three attribute certificates. Each attribute certificate binds the sender name to the corresponding authorization information contained in the field type of the given attribute certificate. This second alternative approach has an advantage in that the four digital certificates can be signed by four independent certificate authorities. On the other hand, the second alternative approach has the disadvantage in that it requires four digital signatures instead of one, and four transactions over a network instead of one when the certificate authority issues the digital certificate to the subject. Thus, the second approach is more computationally expensive and results in more network traffic than the certificate authority issuing a single digital certificate to the subject.

[0011] The present invention seeks to provide an improved digital certificate.

[0012] According to an aspect of the present invention, there is provided a structural digital certificate as specified in claim 1.

[0013] According to another aspect of the present invention, there is provided a method of providing confidentiality of authorisation information as specified in claim 4.

[0014] The preferred embodiments can provide an improved type of digital certificate and corresponding improved methods of employing the digital certificate so that when the sender of a digital certificate presents the digital certificate to the recipient of the digital certificate for a given purpose, only those fields of the digital certificate that have to be inspected by the recipient are revealed to the recipient. The preferred desired digital certificate provides this recipient confidentiality protection without the added computational and network traffic overhead resulting from issuing digital certificates.

[0015] According to the preferred embodiment, there is provided a structured digital certificate for enabling a first recipient of the structured digital certificate to authorize a sender of the structured digital certificate. The structured digital certificate includes a first type field of authorization information relevant to the first recipient and readable by the first recipient. The structured digital certificate includes a first cryptographic folder containing a second type field of authorization information relevant to a second recipient. The second type field of authorization information is not readable by the first recipient.

[0016] In one embodiment, the structured digital certificate includes a second cryptographic folder containing the first type field. In one embodiment, the first type field is not contained in a folder. In one embodiment, there are multiple first type fields in the structured digital certificate.

[0017] In one embodiment, the structured digital certificate includes a sender name and a public key associated with the sender.

[0018] In one embodiment of the present invention, the cryptographic folders of authorization information are structured fields, containing a plurality of nested fields. Each of the plurality of nested fields can be a folder itself. In one embodiment, the digital certificate is an X.509v3 digital certificate. The X.509v3 digital certificate may include extension fields that describe how the certification can be used. The extension fields include one or more criticality flags. In one embodiment the unrelated cryptographic folders contain an encrypted hash value.

[0019] The preferred embodiment also provides a method of providing confidentiality of authorization information in a digital certificate shared by multiple recipients. The method provides cryptographic folders in the digital certificate. At least one first type cryptographic folder contains at least one first type field of authorization information relevant to a first recipient. At least one second type cryptographic folder contains at least one second type field of authorization information relevant to a second recipient. The certificate authority issues the digital certificate by signing the digital certificate and sending the signed digital certificate to the subject. The subject then delivers the signed digital certificate to the first recipient. The at least one first type field of authorization information is readable by the first recipient. The at least one second type field of authorization information is not readable by the first recipient. The first recipient verifies the authenticity of the signed digital certificate.

[0020] According to another aspect of the present invention, there is provided a method of signing a digital certificate at a certificate authority. The method provides cryptographic folders in the digital certificate having authorization information. The certificate authority closes all of the cryptographic folders in the digital certificate. A cryptographic hash of the digital certificate is computed with all folders closed. Digital certificate signature is computed with the computed cryptographic hash of the digital certificate and a private key of the certificate authority.

[0021] In one embodiment, a given cryptographic folder X is closed according to the present invention in the following manner. All of the nested folders in folder X are recursively closed. A cryptographic hash is computed of the contents of folder X including all recursively closed nested folders in folder X. The contents of folder

X are replaced with the computed cryptographic hash of the contents of folder X. A flag is set in the header of folder X to indicate that folder X is closed.

[0022] According to another aspect of the present invention, there is provided a method of delivering a digital certificate from a subject of the digital certificate to a recipient of the digital certificate. The method provides cryptographic folders in the digital certificate having authorization information. A digital certificate signature is transmitted from a certificate authority to the subject of the certificate. An unsigned copy of the digital certificate is transmitted from the certificate authority to the subject of the certificate. Any folders in the unsigned copy of the digital certificate that do not have authorization information relevant to the recipient are closed. The unsigned copy of the digital certificate and the digital certificate signature are transmitted from the subject of the digital certificate to the recipient.

[0023] In one embodiment of the present invention, the step of transmitting a copy of the unsigned digital certificate from the certificate authority to the subject of the certificate is performed over a secure delivery channel. In one embodiment, the secure delivery channel is protected via Internet Protocol Security (IPSEC). In another embodiment, the secure delivery channel is protected by Secure Sockets Layer (SSL).

[0024] According to another aspect of the present invention, there is provided a method of verifying a signature for a digital certificate sent by a subject of the digital certificate to a recipient of the digital certificate. The method provides cryptographic folders in the digital certificate having authorization information. The recipient obtains a public key of the certificate authority corresponding to a private key used by the certificate authority to sign the digital certificate. The recipient closes any of the cryptographic folders left open in the digital certificate by the subject of the digital certificate. The recipient computes a cryptographic hash of the digital certificate. The recipient authenticates the signature for the digital certificate.

[0025] The structured digital certificate and corresponding methods of employing the structural digital certificate according to the described embodiments offer several advantages over conventional digital certificates. A single structured digital certificate according to the present invention can be utilized for multiple, unrelated purposes and still provide recipient confidentiality protection without the added computational and network traffic overhead resulting from sending multiple digital certificates. The hierarchical structure of cryptographic folders utilized within the present invention makes it possible to disclose only those fields of the structured digital certificate that have to be inspected by the recipient for a given specific purpose. Since all but one folder of a structured digital certificate will typically be closed (i.e., contents of the folder replaced with a cryptographic hash), when the digital certificate is transmitted from the sender to the recipient over a network, the time taken to transmit the digital certificate over the network is reduced.

[0026] An embodiment of the present invention is described below, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of an embodiment of structured digital certificate;

Figure 2 is a flowchart illustrating an embodiment of method of providing field confidentiality in digital certificates;

Figure 3A is a flowchart illustrating an embodiment of method of signing structured digital certificates at a certificate authority;

Figure 3B is a flow chart illustrating an embodiment of method of closing a given cryptographic folder X;

Figure 4 is a block and data flow diagram illustrating how a signature is generated for a structured digital certificate at a certificate authority;

Figure 5 is a flowchart illustrating an embodiment of method of delivering a structured digital certificate and corresponding encrypted message to a message recipient;

Figure 6 is a block and data flow diagram illustrating how a structured digital certificate is delivered to a message recipient from a certificate authority, via the subject of the certificate;

Figure 7 is a flowchart illustrating an embodiment of method of verifying the authenticity of a signature of a structured digital certificate;

Figure 8 is a block and data flow diagram illustrating how an embodiment of message recipient verifies the authenticity of a structured digital certificate; and

Figure 9 is a block diagram of a computer system and a corresponding computer readable medium incorporating a function for providing field confidentiality in digital certificates.

[0027] In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural or logical changes may be made without departing from the scope of the claims. The following detailed description, therefore, it not to be taken in a limiting sense.

[0028] Figure 1 is a block diagram of an embodiment of structured digital certificate 30. Structured digital certificate 30 is a data structure, digitally signed by an issuer (i.e., a certificate authority), that includes authorization information about another entity, referred to as a subject (i.e., a sender). The subject of structured digital certificate 30 presents the structured digital certificate to third parties who trust the issuer of structured digital certificate 30. The third parties are referred to as relying parties (i.e., recipients). The relying party computes a

cryptographic hash of the structured digital certificate 30 and uses this hash, together with the public key of the issuer, which is readily available, to verify the digital signature of structured digital certificate 30.

[0029] In one embodiment, structured digital certificate 30 is a basic public key certificate and includes a public key 32 and a sender name 34 associated with the subject of structured digital certificate 30. In another embodiment, structured digital certificate 30 is an extended public key certificate and includes, in addition to public key 32 and sender name 34, additional fields 36, 37 and/or cryptographic folders 38, 40, 42 and 44 which contain authorization information. One example of an extended public key certificate is a X.509v3 certificate, previously described in the Background of the Invention section of the present specification.

[0030] In one embodiment, structured digital certificate 30 includes authorization fields 36 and 37 containing authorization information used for multiple, unrelated purposes. When structured digital certificate 30 is used for one specific purpose, it is desirable to hide the information contained in unrelated fields. One example structured digital certificate 30 can be used to grant access to a UNIX platform and to also grant permission to sign purchase orders. As a result, example structured digital certificate 30 has a first type authorization field 37 that specifies a user ID and a group ID for the UNIX platform, as well as a second type authorization field 36 that specifies a limit on the value of the purchase orders that the subject is authorized to sign. When example structured digital certificate 30 is used to access the UNIX platform, all authorization fields 36 and 37 of structured digital certificate 30 may become visible to the UNIX administrator, such as by being recorded on the system log. However, the UNIX administrator has no need to know the limit on the value of purchase orders as contained in second type authentication field 36. Thus, it is desirable to hide the information contained in second type authentication field 36 when the UNIX administrator examines structured digital certificate 30.

[0031] In one embodiment, an authorization field (or fields) is kept confidential by placing the authorization field in one of the cryptographic folders 38, 40, 42, and 44 and replacing the authorization information of the cryptographic folder with a cryptographic hash of the authorization information. This is accomplished without impairing the ability of the recipient of structured digital certificate 30 to verify the digital signature.

[0032] Cryptographic folders 38, 40, 42 and 44 are each a structured field, containing any number of nested fields. The nested fields can themselves be cryptographic folders. In the illustrated example, structured digital certificate 30 contains four cryptographic folders 38, 40, 42, and 44. Cryptographic folder 42 contains two additional cryptographic folders 46 and 48 along with authorization field 50. Cryptographic folder 48 contains one additional cryptographic folder 52 along with authorization field 54.

[0033] In one embodiment, cryptographic folders 38, 40, 42, 44, 46, 48, and 52 can be in one of two states, open or closed. The current state is indicated by a flag in the header of the cryptographic folder. In X.509v3 digital certificates, each extension (i.e., authorization) field has a criticality flag. The criticality flag is employed in situations where a recipient (i.e., relying party) is presented with one or more extension fields that it does not understand, perhaps because the extension is newer than the computer program used by the relying party. If the criticality flag is not set, the relying party can ignore the unknown extension. If the criticality flag is set, the relying party rejects structured digital certificate 30.

[0034] Cryptographic folders provide for increased flexibility in the use of criticality flags, but the interaction of cryptographic folders and criticality flags must be handled cautiously. An authorization field is defined recursively as being visible if it is not inside a cryptographic folder or if it is inside an open cryptographic folder which is itself visible. An application must reject a digital certificate if it contains a visible field where the criticality flag is set.

[0035] The issuer of the structure digital certificate 30 must ensure that a critical field is not placed inside an irrelevant cryptographic folder. Thus, if a critical field is relevant to a relying party, then, in the folder hierarchy, every cryptographic folder containing the authorization field must also be relevant to that relying party. These cryptographic folders must be open when the structured digital certificate 30 is presented to the relying party, and the critical authentication field must be visible.

[0036] **FIG. 2** is a flowchart of a method illustrated generally at 100 for providing field confidentiality in structured digital certificates, such as the structured digital certificate 30 illustrated in **FIG. 1.** At block 102, method 100 begins by signing structured digital certificate 30 at a certificate authority. The certificate authority (i.e., issuer) of structured digital certificate 30 closes all cryptographic folders within the structured digital certificate in order to generate a signature for the structured digital certificate. The method step indicated at block 102 for signing the structured digital certificate 30 is described in greater detail in reference to **FIG. 3A.**

[0037] After structured digital certificate 30 has been signed at block 102, the digital certificate signature and a copy of the digital certificate with at least one cryptographic open folder is delivered to the recipient via the subject of the digital certificate, as indicated at block 104. Only authorization information relevant to the recipient is visible to the recipient within the signed digital certificate (i.e., via open folders). The method step indicated at block 104 for delivering the structured digital certificate 30 to the recipient is described in greater detail in reference to **FIG. 5.**

[0038] Upon receipt of the signed structured digital certificate 30, the recipient verifies the authenticity of the signed digital certificate, as indicated at block 106. Before verifying the signed digital certificate, the recipient

closes any cryptographic folders that are left open by the subject of the digital certificate. Thus, the relying party is able to perform the signature verification independently of the state of the cryptographic folders in the copy of the structured digital certificate presented by the subject. The method step indicated at block 106 for verifying the authenticity of the structured digital certificate 30 is described in greater detail in reference to **FIG. 7.**

[0039] **FIG. 3A** is a flowchart illustrating one embodiment of a method 102 for signing structured digital certificates 30 at a certificate authority. As stated previously, before structured digital certificate 30 is signed or verified, any cryptographic folders present within structured digital certificate 30 are closed. Method 102 begins by closing all of the cryptographic folders in structured digital certificate 30, as indicated at block 110. Next, a cryptographic hash of the structured digital certificate 30 is computed, as indicated at block 112. The cryptographic hash can be computed by a variety of methods. In one embodiment, the cryptographic hash is computed by SHA-1. At block 114, the digital certificate signature is computed with the computed cryptographic hash of the digital certificate and a private key of the certificate authority.

[0040] **Fig. 3B** is a flow chart illustrating one embodiment of a method 115 for closing a cryptographic folder X. As indicted at block 116, all of the nested folders in folder X are recursively closed. As indicated at block 117, a cryptographic hash is computed of the contents of folder X including all recursively closed nested folders in folder X. As indicated at block 118, the contents of folder X are replaced with the computed cryptographic hash of the contents of folder X. As indicated at block 119, a flag is set in the header of folder X to indicate that folder X is closed.

[0041] **FIG. 4** is a block and data flow diagram illustrating an operation 118, where a signature is generated for structured digital certificate 30 at the certificate authority. As indicated at block 110 of **FIG. 3A,** all cryptographic folders within structured digital certificate 30 must be closed before a signature can be generated. In operation 118, the authorization information contents of open cryptographic folder 52 (i.e., the lowest level cryptographic folder within the hierarchy of cryptographic folders) is replaced with a cryptographic hash value, and cryptographic folder 52 is closed, as indicated at 120 in **FIG. 4.** Next, the authorization information contents of open cryptographic folders 46 and 48 are replaced with corresponding cryptographic hash values, and cryptographic folders 46 and 48 are closed, as indicated at 122. The authorization information contents of open top-level cryptographic folders 38, 40, 42, and 44 within structured digital certificate 30 are then replaced with corresponding cryptographic hash values, and cryptographic folders 38, 40, 42 and 44 are closed, as indicated at 124. At this point, the hierarchy of cryptographic folders within structured digital certificate 30 have been "flattened" such that a signature can be generated for the structured digital certificate 30, as indicated at 126.

[0042] **FIG. 5** is a flowchart illustrating one embodiment of a method 104 for delivering structured digital certificate 30 to a recipient of the digital certificate. Method 104 begins by transmitting the digital certificate signature from the certificate authority (i.e., issuer) to the subject of the digital certificate, as indicated at block 130. At block 132, a copy of the unsigned digital certificate is transmitted from the certificate authority to the subject of the digital certificate. The subject of the digital certificate then closes any cryptographic folders in the copy of the unsigned digital certificate that the recipient does not need to see (i.e., folders do not contain authorization information relevant to the message recipient), as indicated at block 134. Finally the copy of the unsigned digital certificate and the digital certificate signature generated by the certificate authority are transmitted from the subject of the digital certificate to the recipient of the digital certificate, as indicated at block 136.

[0043] **FIG. 6** is a block and data flow diagram illustrating an operation 150 where a structured digital certificate signed by a certificate authority is delivered to a recipient, via the subject of the certificate. As described previously, certificate authority 152 closes all of the cryptographic folders within structured digital certificate 30 before signing structured digital certificate 30. After the structured digital certificate has been signed, digital certificate signature126 is delivered to a subject 154 of the digital certificate. In addition to the digital certificate signaturel26, certificate authority 152 also delivers a copy of the structured digital certificate 158 where all of the cryptographic folders are open to the subject 154 of the digital certificate. If the copy of the structured digital certificate 158 contains sensitive information, then it becomes necessary to provide security to a delivery channel 159 between certificate authority 152 and the subject 154 of the certificate. In one embodiment, delivery channel 159 is secured by Internet Protocol Security (IPSEC). In an alternate embodiment, delivery channel 159 is secured by Secure Sockets Layer (SSL).

[0044] Subject 154 of the digital certificate forwards the digital certificate signature 126 to recipient 156. Before submitting the copy of the structured digital certificate 158 to recipient 156, subject 154 of the digital certificate closes any cryptographic folders that recipient 156 does not need to see, as indicated at 160.

[0045] **FIG. 7** is a flowchart illustrating one embodiment of a method 106 for verifying the authenticity of a signature of a structured digital certificate 30. In method 106, recipient 156 obtains a public key of the certificate authority 152 corresponding to a private key used by the certificate authority to sign the digital certificate, which is made readily available by certificate authority 152, as indicated at block 178. Method 106 closes any cryptographic folders left open in the copy of the structured digital certificate by subject 154 of the digital certificate, as indicated at block 180. As indicated at block 182, recipient 156 computes a cryptographic hash of the struc-

tured digital certificate 158 with all folders closed. As indicated at block 184, recipient 156 verifies the signature for the digital certificate with the public key and the computed cryptographic hash of the digital certificate.

[0046] **FIG. 8** is a block and data flow diagram illustrating an operation 210 where a message recipient verifies the authenticity of a structured digital certificate. In operation 210, recipient 156 obtains a public key 214 of the certificate authority 152, as indicated at 178. Before verifying signed digital certificate 126, recipient 156 closes all cryptographic folders that were left open by the subject 154 of the certificate 154 in the copy of the digital certificate 160, as indicated at block 180. As indicated at block 182, recipient 156 computes a cryptographic hash 216 of the digital certificate 212 having all cryptographic folders closed. As indicated at block 184, recipient 156 verifies the signature of the digital certificate 126 with the public key 214 and the computed cryptographic hash 216 of the digital certificate.

[0047] **FIG. 9** illustrates one embodiment of a computer system 250 and an external computer readable medium 252 which can be employed to provide field confidentiality in digital certificates at a certificate authority to incorporate a method of signing a digital certificate; at a subject of the digital certificate to incorporate a method of delivering the digital certificate from the subject to a recipient of the digital certificate; or at the recipient of the digital certificate to incorporate a method of verifying a signature for the digital certificate. Embodiments of external computer readable medium 252 include, but are not limited to: a CD-ROM, a floppy disk, and a disk cartridge. Any one of the above methods for providing field confidentiality in digital certificates can be implemented in a variety of compiled and interpreted computer languages. External computer readable medium 252 stores source code, object code, executable code, shell scripts and/or dynamic link libraries for any one of the above methods for providing field confidentiality in digital certificates. An input device 254 reads external computer readable medium 252 and provides this data to computer system 250. Embodiments of input device 254 include but are not limited to: a CD-ROM reader, a floppy disk drive, and a data cartridge reader.

[0048] Computer system 250 includes a central processing unit 256 for executing any one of the above methods for providing field confidentiality in digital certificates. Computer system 250 also includes local disk storage 262 for locally storing any one of the above methods for providing field confidentiality in digital certificates before, during and after execution. Any one of the above methods for providing field confidentiality in digital certificates also utilizes memory 260 within the computer system during execution. Upon execution of any one of the above methods for providing field confidentiality in digital certificates, output data is produced and directed to an output device 258. Embodiments of output device 258 include, but are not limited to: a computer display device, a printer, and/or a disk storage device.

[0049] A method is provided by which the subject (i. e., sender) of a digital certificate can keep certain fields within the digital certificate confidential as the sender presents the digital certificate to a relying party (i.e., recipient). This specific field confidentiality is accomplished through a structured digital certificate which includes a hierarchical structure of cryptographic folders. In addition to providing field confidentiality, the described embodiments can improve the speed of signature verification by the receiving party, reduce network traffic, and reduce computational overhead.

[0050] The disclosures in United States patent application no. 09/483,189, from which this application claims priority, and in the abstract accompanying this application are incorporated herein by reference.

Claims

1. A structured digital certificate (30) for enabling a first recipient of the structured digital certificate to authorize a sender of the structured digital certificate, the structured digital certificate comprising:

   a first type of authorization (87) relevant to the first recipient and readable by the first recipient; and
   a first cryptographic folder (38-44) containing a second type field of authorization information (36) relevant to a second recipient and readable by the second recipient, wherein the second type field of authorization information is not readable by the first recipient.

2. A digital certificate as in claim 1, comprising one or more of:

   a second cryptographic folder (38-44) containing the first type field;
   multiple type fields (37);
   a sender name; and/or
   a public key associated with the sender.

3. A digital certificate as in claim 1 or 2, wherein the first type field (37) is not contained in a cryptographic folder (38-44).

4. A method of providing confidentiality of authorization information in a digital certificate shared by multiple recipients, the method comprising the steps of:

   providing cryptographic folders (38-44) in the digital certificate, wherein at least one first type cryptographic folder contains at least one second type cryptographic folder (36) contains at least one second type field of authorization information relevant to a second recipient;

issuing and the digital certificate (30) at a certificate authority by signing the digital certificate and sending the signed digital certificate to a subject;
delivering the signed digital certificate from the subject to the first recipient, wherein the at least one first type field of authorization information (37) is readable by the first recipient, and the at least one second type field of authorization information (36) is not readable by the first recipient; and
verifying the authenticity of the signed digital certificate (30) by the first recipient.

5. A method as in claim 4, comprising one or more of the following:

(a) the step of signing the digital certificate at a certificate authority comprises the steps of closing all of the cryptographic folders in the digital certificate computing a cryptographic hash of the digital certificate and computing a digital certificate signature with computed cryptographic hash of the digital certificate and a private key of the certificate authority;
(b) the step of delivering the signed digital certificate to the first recipient includes the steps of closing any cryptographic folders in the copy of the unsigned digital certificate that do not have at least one first type field of authorization information and transmitting the copy of the unsigned digital certificate and the digital certificate signature from the subject of the digital certificate to the first recipient; and
(c) the step of verifying the authenticity of the digital certificate by the first recipient includes obtaining a public key from the certificate authority, closing any cryptographic folders left open in the unsigned digital certificate, computing a cryptographic hash of the unsigned digital certificate with all folders closed and verifying the signature of the digital certificate with the public key and the computed cryptographic hash of the unsigned digital certificate.

6. A method of signing a digital certificate at a certificate authority, the method comprising the steps of:

providing cryptographic folders (38-44) in the digital certificate (30) having authorization information;
closing all of the cryptographic folders in the digital certificate;
computing a cryptographic hash of the digital certificate (30); and
computing a digital certificate signature with the computed cryptographic hash of the digital certificate and a private key of the certificate authority.

7. A method as in claim 6, wherein the step of closing all of the cryptographic folders (38-44) in the digital certificate (30) includes closing a cryptographic folder X according to the following steps:

recursively closing all nested folders in folder X;
computing the cryptographic hash of the contents of folder X;
replacing the contents of folder X with the computed cryptographic hash of the contents of folder X; and
setting a flag in a header of folder X to indicate that folder X is closed.

8. A method of delivering a digital certificate from a subject of the digital certificate to a recipient of the digital certificate, the method comprising the steps of:

providing cryptographic folders (38-44) in the digital certificate (30) having authorization information;
transmitting a digital certificate signature from a certificate authority to the subject of the certificate;
transmitting an unsigned copy of the digital certificate (30) from the certificate authority to the subject of the certificate;
closing any folders (38-44) in the unsigned copy of the digital certificate that do not have authorization information relevant to the recipient; and
transmitting the unsigned copy of the digital certificate and the digital certificate signature from the subject of the digital certificate to the recipient.

9. A method of verifying a signature for a digital certificate (30) sent by a subject of the digital certificate to a recipient of the digital certificate, the method comprising the steps of:

providing cryptographic folders (38-44) in the digital certificate (30) having authorization information;
obtaining a public key of the certificate authority corresponding to a private key used by the certificate authority to sign the digital certificate (30);
closing any of the cryptographic folders (38-44) left open in the digital certificate (30) by the subject of the digital certificate;
computing a cryptographic hash of the digital certificate (30) with all cryptographic folders closed; and
verifying the signature for the digital certificate

with the public key and the computed cryptographic hash of the digital certificate.

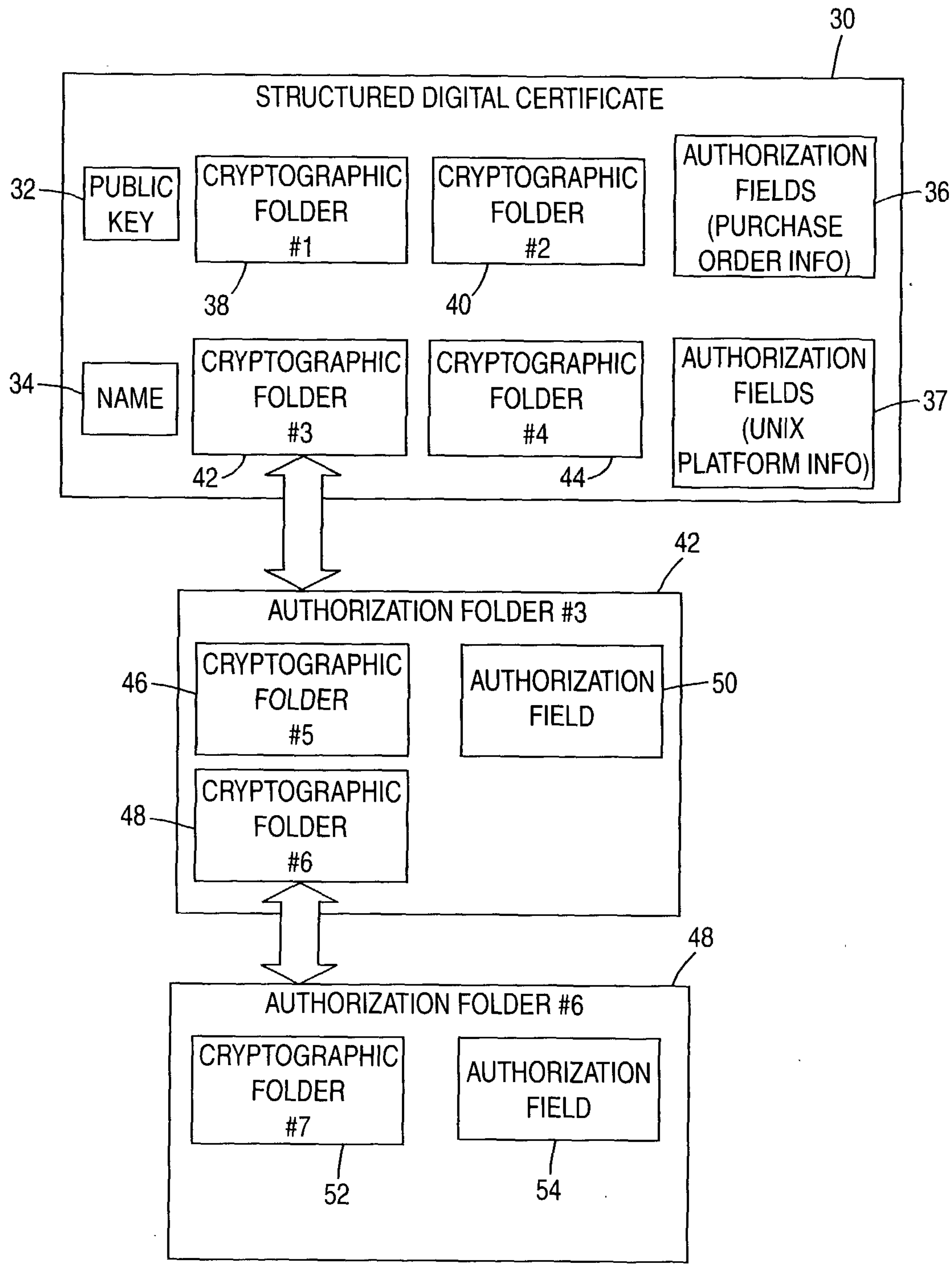
30
STRUCTURED DIGITAL CERTIFICATE
32
PUBLIC KEY
CRYPTOGRAPHIC FOLDER #1
CRYPTOGRAPHIC FOLDER #2
AUTHORIZATION FIELDS (PURCHASE ORDER INFO)
36
38
40
34
NAME
CRYPTOGRAPHIC FOLDER #3
CRYPTOGRAPHIC FOLDER #4
AUTHORIZATION FIELDS (UNIX PLATFORM INFO)
37
42
44
42
AUTHORIZATION FOLDER #3
46
CRYPTOGRAPHIC FOLDER #5
AUTHORIZATION FIELD
50
48
CRYPTOGRAPHIC FOLDER #6
48
AUTHORIZATION FOLDER #6
CRYPTOGRAPHIC FOLDER #7
AUTHORIZATION FIELD
52
54

Fig. 1

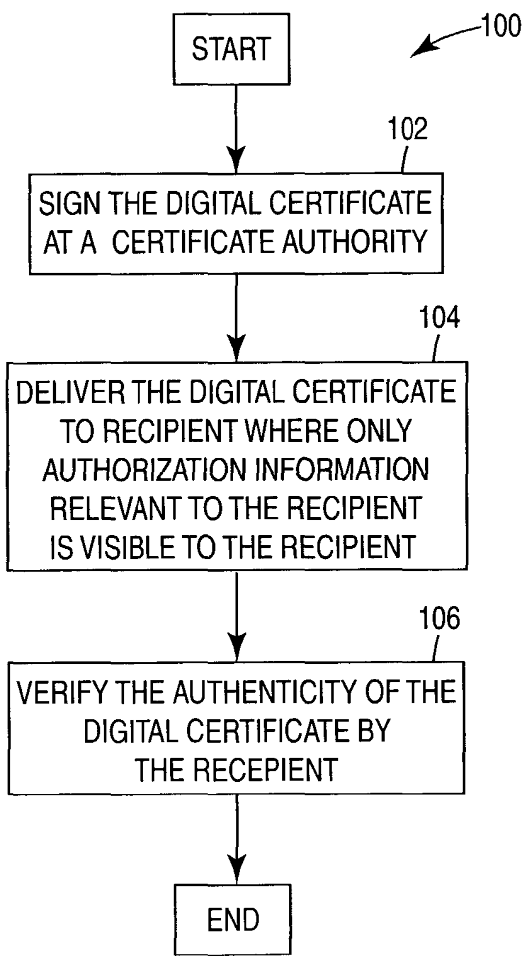
100
START
102
SIGN THE DIGITAL CERTIFICATE AT A CERTIFICATE AUTHORITY
104
DELIVER THE DIGITAL CERTIFICATE TO RECIPIENT WHERE ONLY AUTHORIZATION INFORMATION RELEVANT TO THE RECIPIENT IS VISIBLE TO THE RECIPIENT
106
VERIFY THE AUTHENTICITY OF THE DIGITAL CERTIFICATE BY THE RECEPIENT
END

Fig. 2

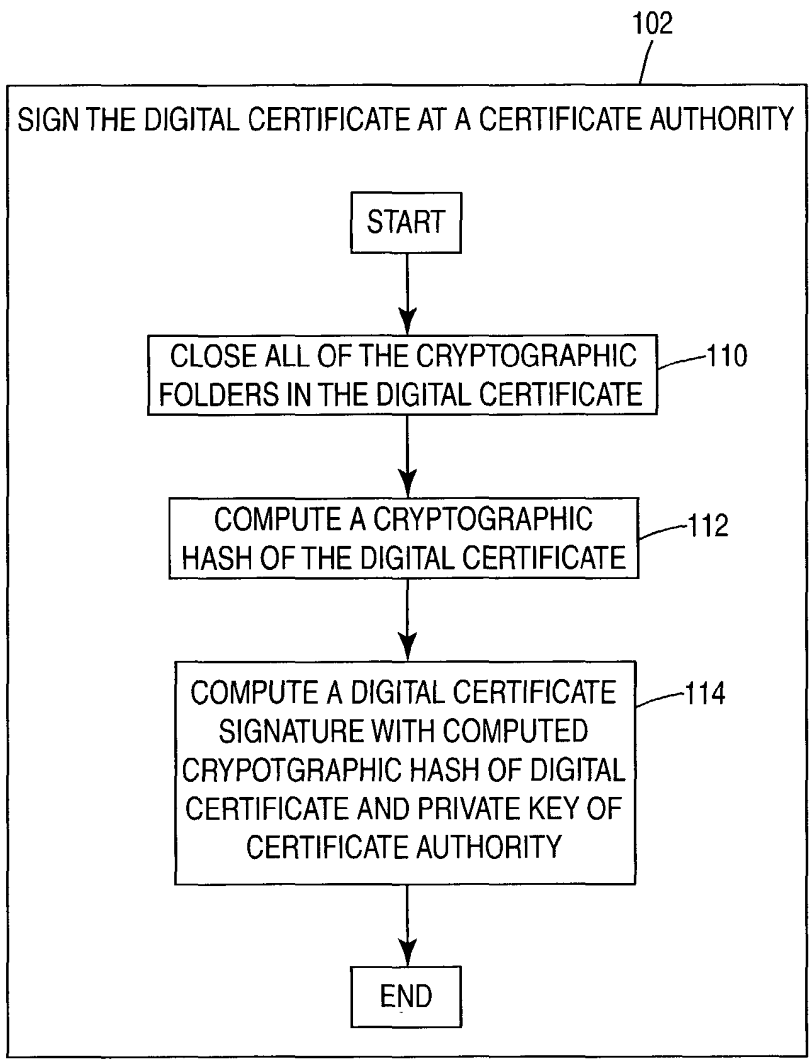
102
SIGN THE DIGITAL CERTIFICATE AT A CERTIFICATE AUTHORITY
START
CLOSE ALL OF THE CRYPTOGRAPHIC FOLDERS IN THE DIGITAL CERTIFICATE
110
COMPUTE A CRYPTOGRAPHIC HASH OF THE DIGITAL CERTIFICATE
112
COMPUTE A DIGITAL CERTIFICATE SIGNATURE WITH COMPUTED CRYPOTGRAPHIC HASH OF DIGITAL CERTIFICATE AND PRIVATE KEY OF CERTIFICATE AUTHORITY
114
END

Fig. 3A

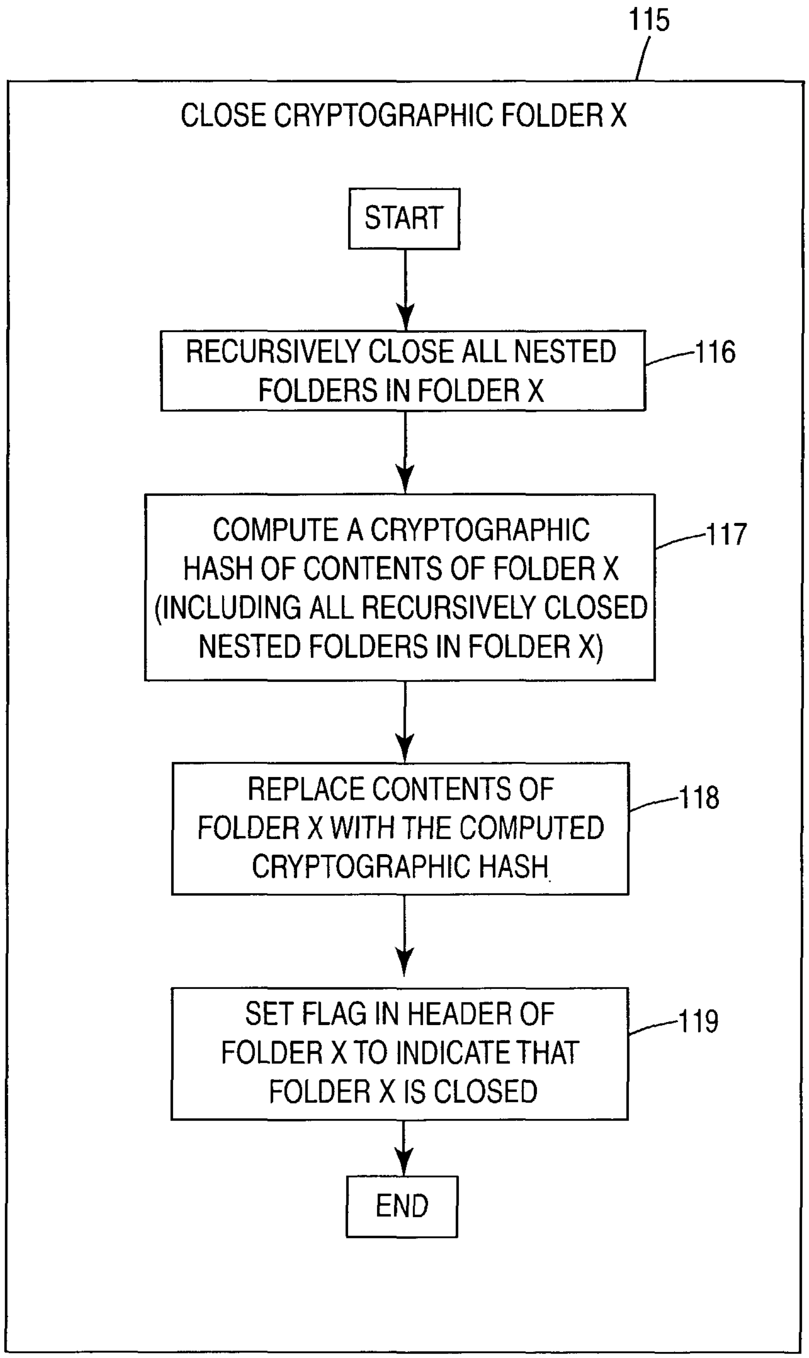
115
CLOSE CRYPTOGRAPHIC FOLDER X
START
RECURSIVELY CLOSE ALL NESTED FOLDERS IN FOLDER X
116
COMPUTE A CRYPTOGRAPHIC HASH OF CONTENTS OF FOLDER X (INCLUDING ALL RECURSIVELY CLOSED NESTED FOLDERS IN FOLDER X)
117
REPLACE CONTENTS OF FOLDER X WITH THE COMPUTED CRYPTOGRAPHIC HASH
118
SET FLAG IN HEADER OF FOLDER X TO INDICATE THAT FOLDER X IS CLOSED
119
END

Fig. 3B

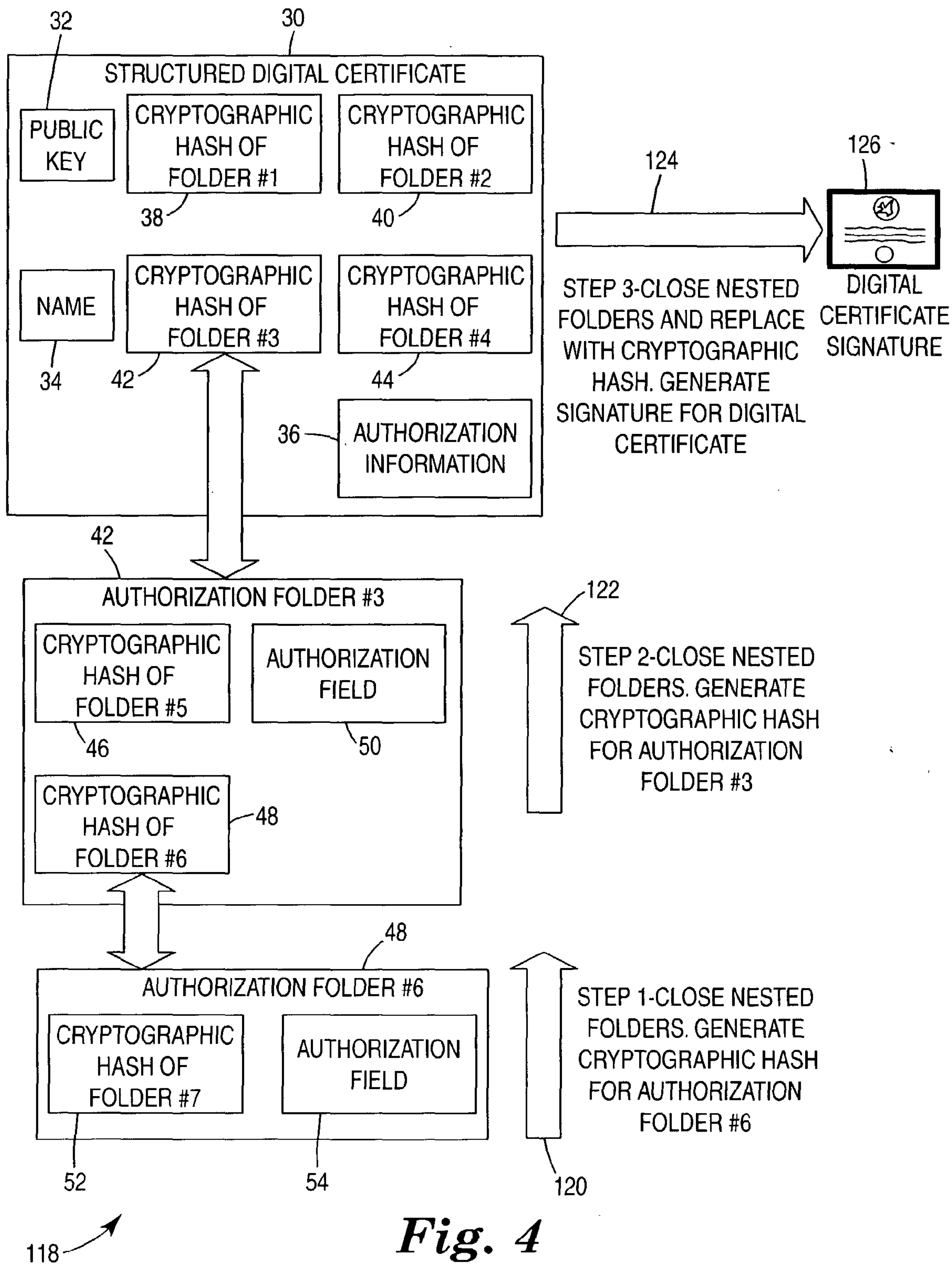
32
30
STRUCTURED DIGITAL CERTIFICATE
PUBLIC KEY
CRYPTOGRAPHIC HASH OF FOLDER #1
CRYPTOGRAPHIC HASH OF FOLDER #2
38
40
124
126
NAME
CRYPTOGRAPHIC HASH OF FOLDER #3
CRYPTOGRAPHIC HASH OF FOLDER #4
34
42
44
36
AUTHORIZATION INFORMATION
STEP 3-CLOSE NESTED FOLDERS AND REPLACE WITH CRYPTOGRAPHIC HASH. GENERATE SIGNATURE FOR DIGITAL CERTIFICATE
DIGITAL CERTIFICATE SIGNATURE
42
AUTHORIZATION FOLDER #3
CRYPTOGRAPHIC HASH OF FOLDER #5
AUTHORIZATION FIELD
46
50
122
STEP 2-CLOSE NESTED FOLDERS. GENERATE CRYPTOGRAPHIC HASH FOR AUTHORIZATION FOLDER #3
CRYPTOGRAPHIC HASH OF FOLDER #6
48
48
AUTHORIZATION FOLDER #6
CRYPTOGRAPHIC HASH OF FOLDER #7
AUTHORIZATION FIELD
STEP 1-CLOSE NESTED FOLDERS. GENERATE CRYPTOGRAPHIC HASH FOR AUTHORIZATION FOLDER #6
52
54
120
118

Fig. 4

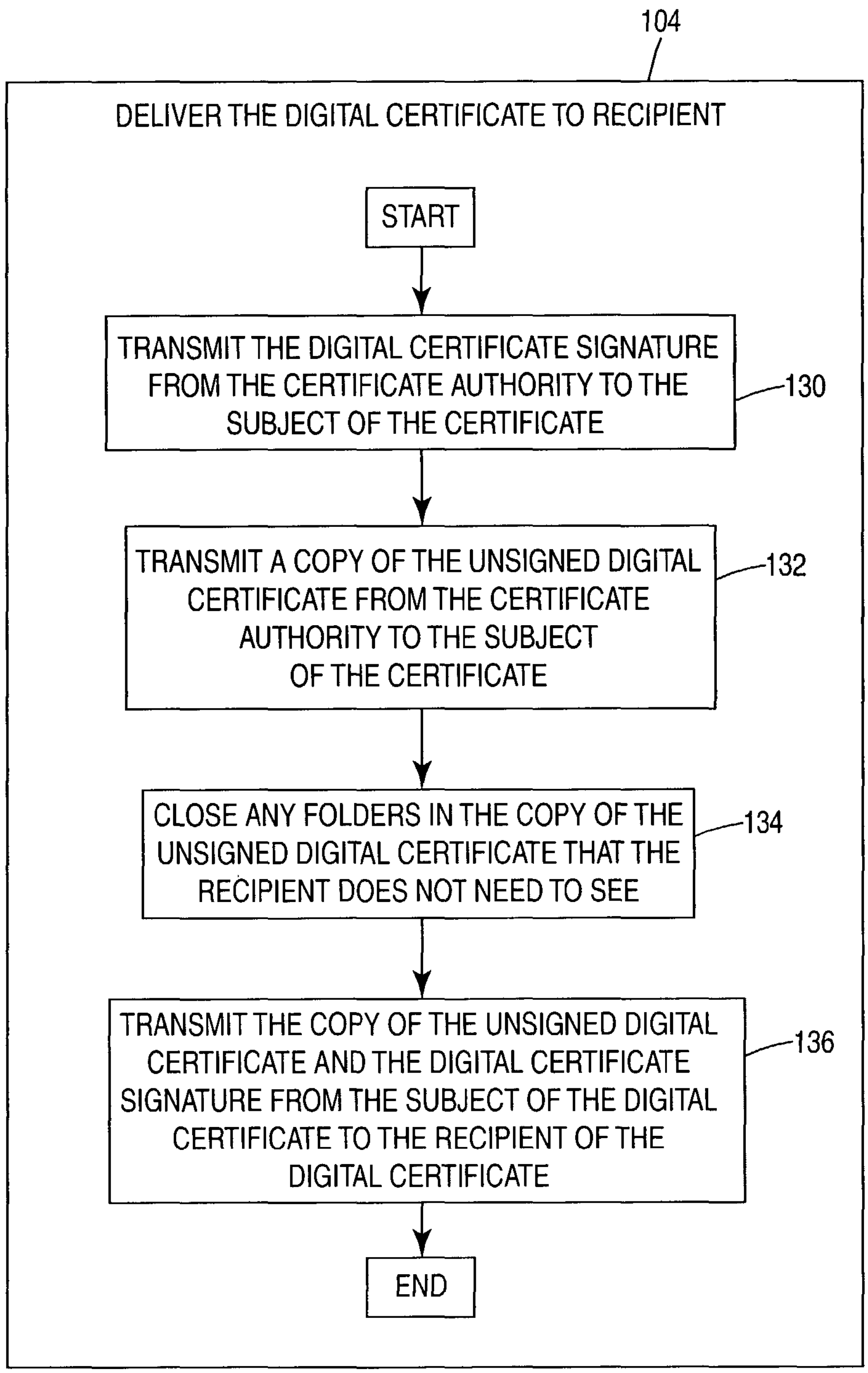
104
DELIVER THE DIGITAL CERTIFICATE TO RECIPIENT
START
TRANSMIT THE DIGITAL CERTIFICATE SIGNATURE FROM THE CERTIFICATE AUTHORITY TO THE SUBJECT OF THE CERTIFICATE
130
TRANSMIT A COPY OF THE UNSIGNED DIGITAL CERTIFICATE FROM THE CERTIFICATE AUTHORITY TO THE SUBJECT OF THE CERTIFICATE
132
CLOSE ANY FOLDERS IN THE COPY OF THE UNSIGNED DIGITAL CERTIFICATE THAT THE RECIPIENT DOES NOT NEED TO SEE
134
TRANSMIT THE COPY OF THE UNSIGNED DIGITAL CERTIFICATE AND THE DIGITAL CERTIFICATE SIGNATURE FROM THE SUBJECT OF THE DIGITAL CERTIFICATE TO THE RECIPIENT OF THE DIGITAL CERTIFICATE
136
END

Fig. 5

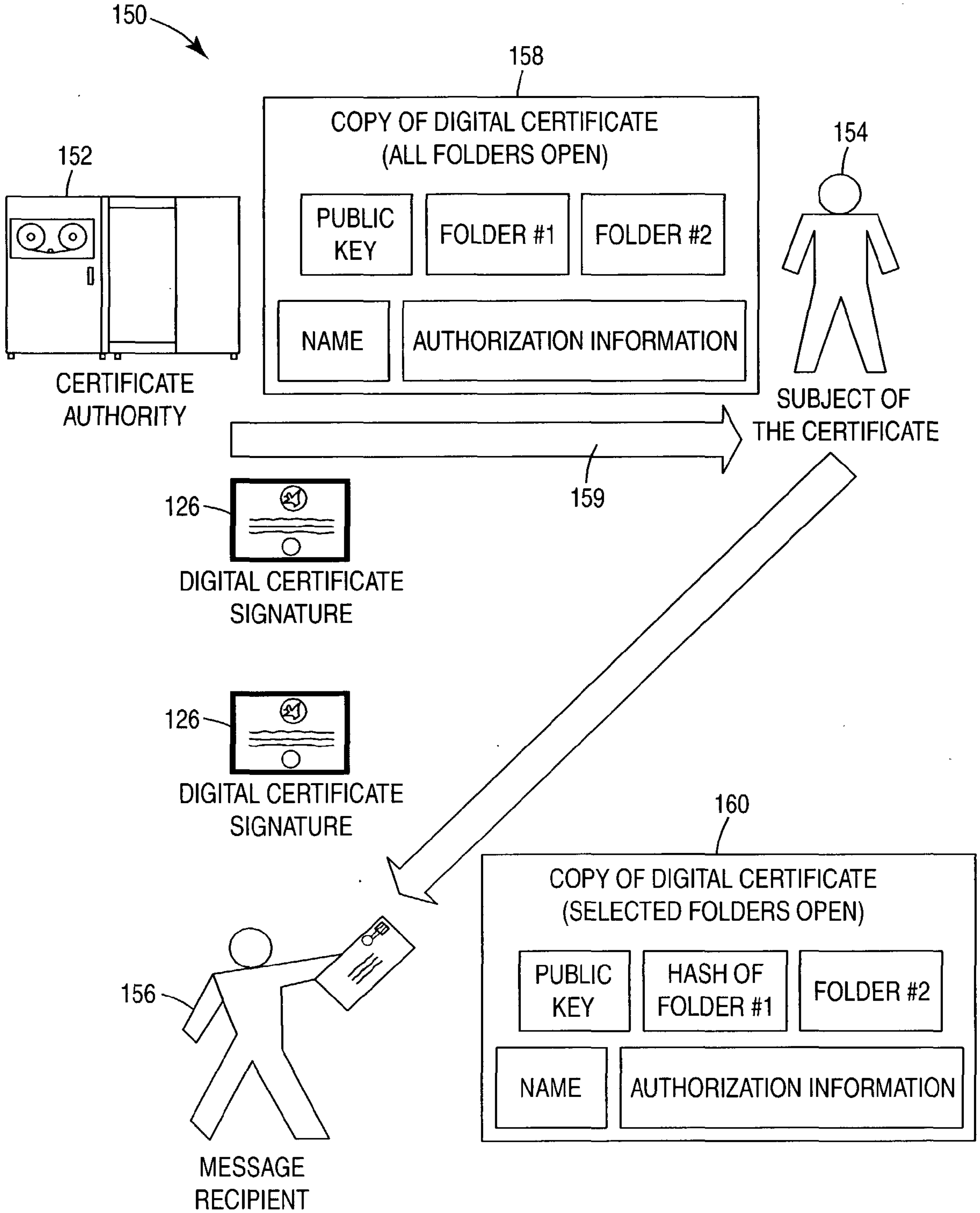
150
158
COPY OF DIGITAL CERTIFICATE
(ALL FOLDERS OPEN)
PUBLIC KEY
FOLDER #1
FOLDER #2
NAME
AUTHORIZATION INFORMATION
152
CERTIFICATE AUTHORITY
154
SUBJECT OF THE CERTIFICATE
159
126
DIGITAL CERTIFICATE SIGNATURE
126
DIGITAL CERTIFICATE SIGNATURE
160
COPY OF DIGITAL CERTIFICATE
(SELECTED FOLDERS OPEN)
PUBLIC KEY
HASH OF FOLDER #1
FOLDER #2
NAME
AUTHORIZATION INFORMATION
156
MESSAGE RECIPIENT

Fig. 6

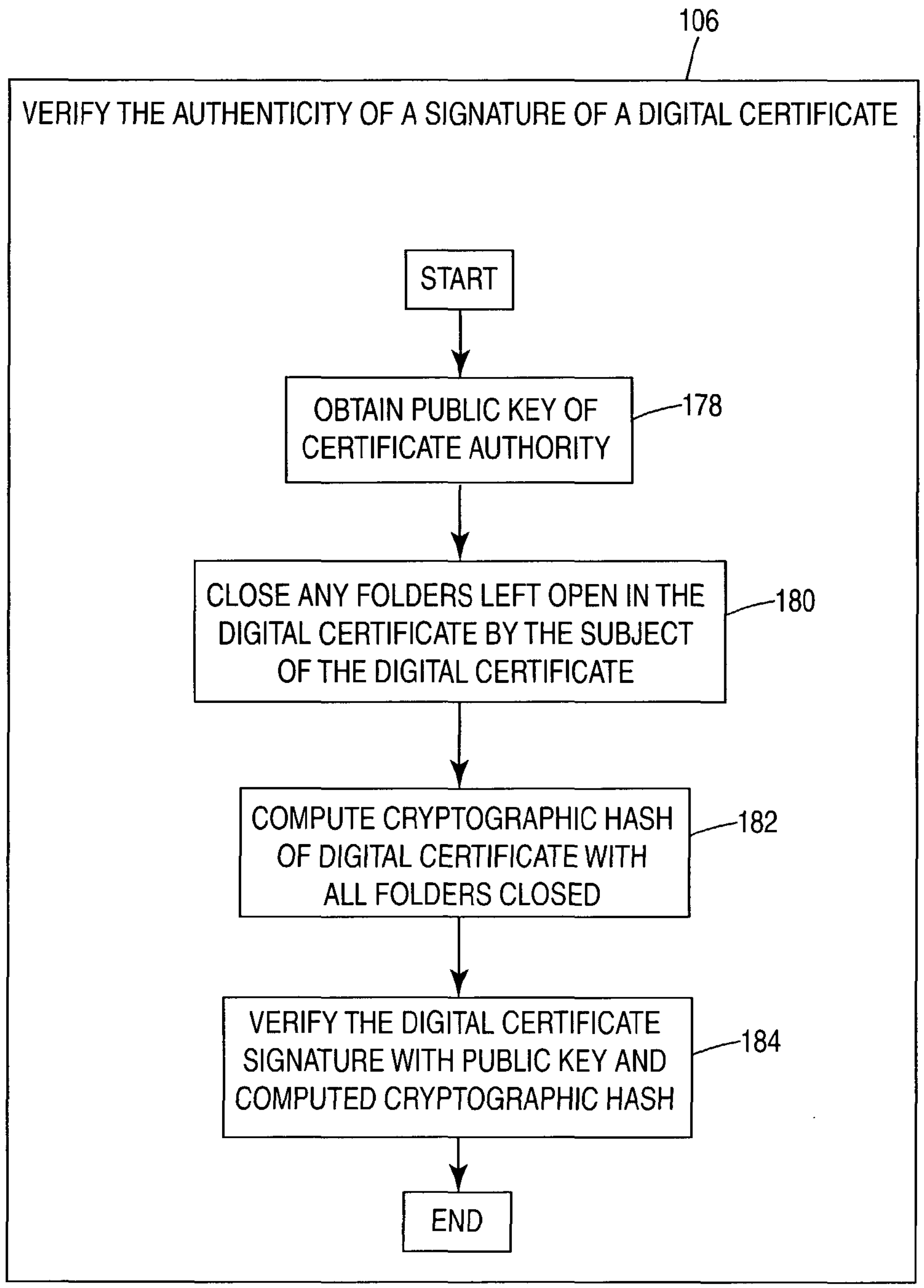
106
VERIFY THE AUTHENTICITY OF A SIGNATURE OF A DIGITAL CERTIFICATE
START
OBTAIN PUBLIC KEY OF CERTIFICATE AUTHORITY
178
CLOSE ANY FOLDERS LEFT OPEN IN THE DIGITAL CERTIFICATE BY THE SUBJECT OF THE DIGITAL CERTIFICATE
180
COMPUTE CRYPTOGRAPHIC HASH OF DIGITAL CERTIFICATE WITH ALL FOLDERS CLOSED
182
VERIFY THE DIGITAL CERTIFICATE SIGNATURE WITH PUBLIC KEY AND COMPUTED CRYPTOGRAPHIC HASH
184
END

Fig. 7

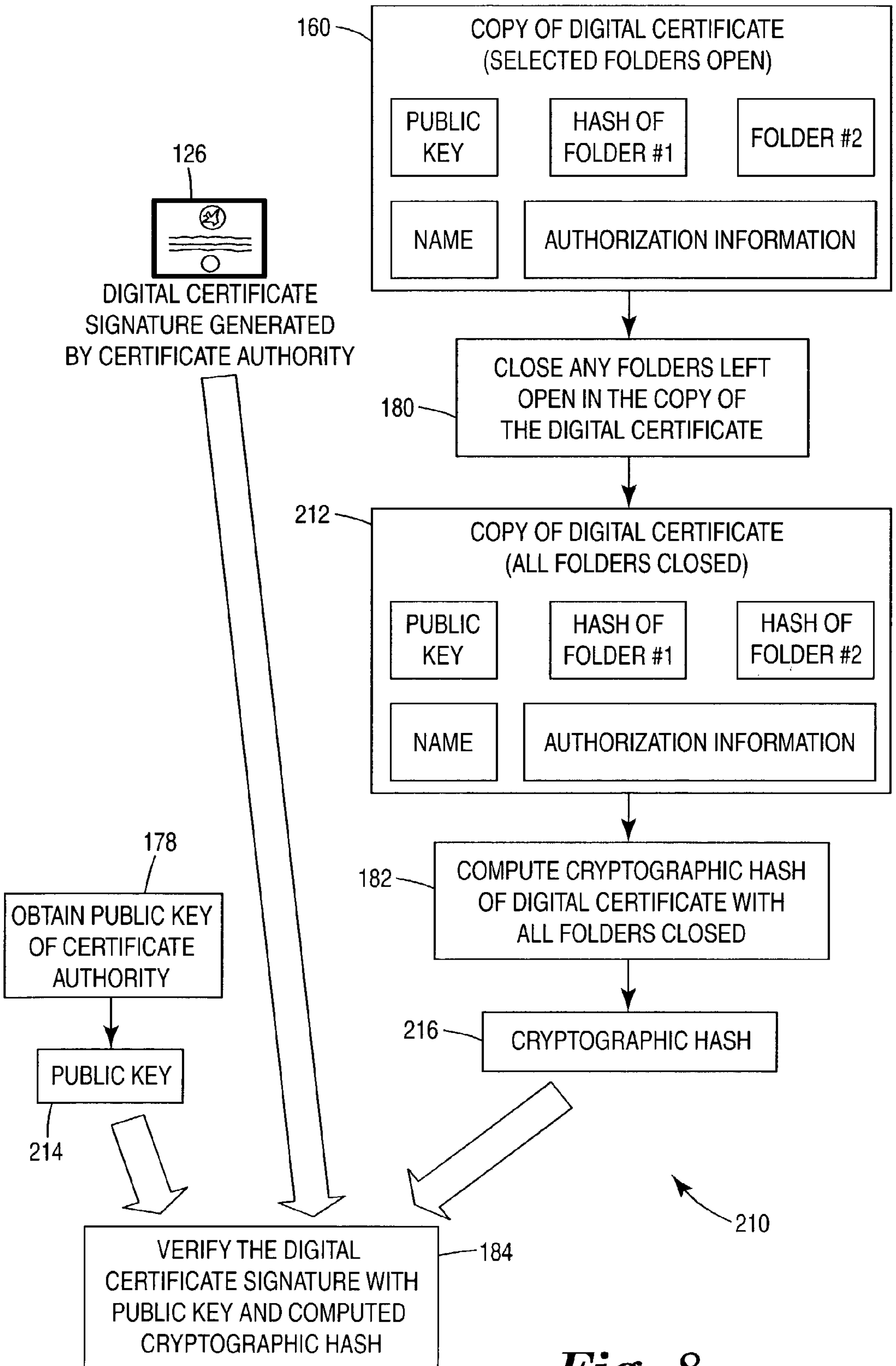
160
COPY OF DIGITAL CERTIFICATE (SELECTED FOLDERS OPEN)
PUBLIC KEY
HASH OF FOLDER #1
FOLDER #2
NAME
AUTHORIZATION INFORMATION
126
DIGITAL CERTIFICATE SIGNATURE GENERATED BY CERTIFICATE AUTHORITY
180
CLOSE ANY FOLDERS LEFT OPEN IN THE COPY OF THE DIGITAL CERTIFICATE
212
COPY OF DIGITAL CERTIFICATE (ALL FOLDERS CLOSED)
PUBLIC KEY
HASH OF FOLDER #1
HASH OF FOLDER #2
NAME
AUTHORIZATION INFORMATION
178
OBTAIN PUBLIC KEY OF CERTIFICATE AUTHORITY
182
COMPUTE CRYPTOGRAPHIC HASH OF DIGITAL CERTIFICATE WITH ALL FOLDERS CLOSED
PUBLIC KEY
214
216
CRYPTOGRAPHIC HASH
210
VERIFY THE DIGITAL CERTIFICATE SIGNATURE WITH PUBLIC KEY AND COMPUTED CRYPTOGRAPHIC HASH
184

Fig. 8

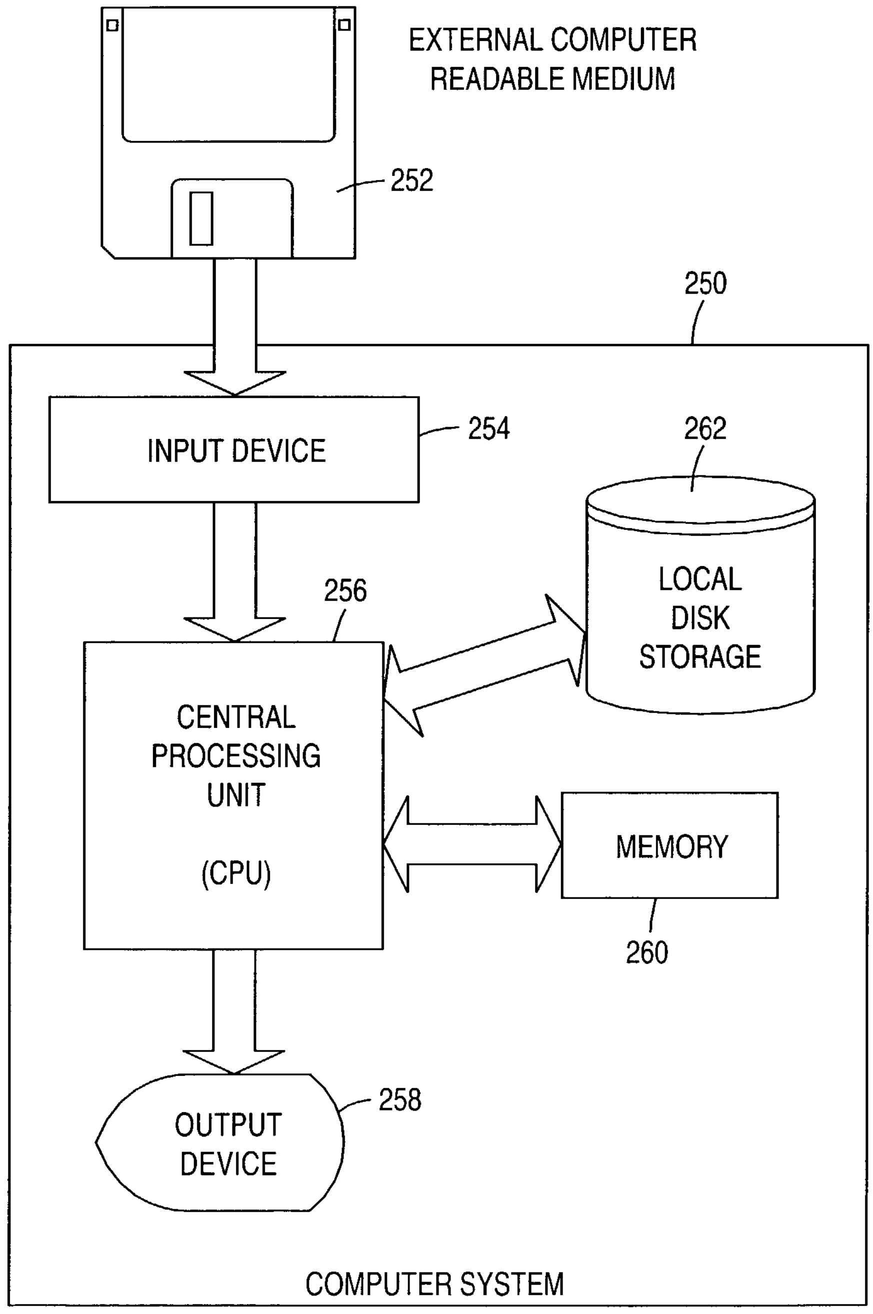
EXTERNAL COMPUTER
READABLE MEDIUM
252
250
INPUT DEVICE
254
262
256
LOCAL
DISK
STORAGE
CENTRAL
PROCESSING
UNIT
(CPU)
MEMORY
260
258
OUTPUT
DEVICE
COMPUTER SYSTEM

Fig. 9